Countering Violent Extremism Online and Offline

Susan Szmania
University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism (START)
Department of Homeland Security

Phelix Fincher
Department of Homeland Security

In the wake of devastating attacks by violent extremists around the world, policy makers have invested considerable effort into understanding terrorists' use of the Internet as they radicalize and mobilize to violence. To that end, the article "Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes" by Paul Gill, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan (2017, this issue) contributes important data to a timely policy discussion. The authors' central finding, "that there is no easy offline versus online violent radicalization dichotomy to be drawn," highlights a gap in our current conceptualization of the radicalization process and suggests several implications, particularly for countering violent extremism (CVE) policies and programs.

Implications for Countering Violent Extremism

CVE has risen to prominence as a policy goal, not only for national governing bodies but also for international institutions like the United Nations (UN). In 2015, the UN issued its *Plan of Action to Prevent Violent Extremism*, which recognizes that "counter-terrorism measures have not been sufficient to prevent the spread of violent extremism" (p. 2). Instead, CVE aims to "prevent the pull of terrorist recruitment and influence by building resilience among populations vulnerable to radicalization" (Holmer, 2013: 2). In the United States, federal CVE guidance has stressed the role of empowering communities to develop and implement locally tailored prevention and intervention programs to address violent extremism. In Europe, including in the United Kingdom, CVE efforts have been described

 Direct correspondence to Susan Szmania, 8400 Baltimore Avenue, College Park, Maryland 20740 (e-mail: sszmania@umd.edu).

DOI:10.1111/1745-9133.12267

as more "comprehensive," "ambitious," and focused on "individual interventions" (Vidino and Hughes, 2015: 1).

Among international policy makers, recent attention has been given to whether CVE prevention and intervention programs are effective, leading to calls for more evidence-based research and program evaluation (Mastroe and Szmania, 2016). Providing clear metrics for CVE programs remains a top priority on both sides of the Atlantic, not only to justify government program expenditures but also to provide safety and security to citizens. To that end, the current study offers specific insights about online behaviors that lead to violence, which ideally can be translated into evidence to build intervention programs and policies.

Prevention Efforts Online and Offline

As Gill et al. (2017) point out, policy makers have often conceptualized online and offline radicalizing environments as separate and distinct. Such a distinction was present, for example, after the horrific tragedy in Orlando, Florida, where Omar Mateen killed 49 people in a nightclub. Public statements by the White House and the Federal Bureau of Investigation concluded that the killer was "strongly radicalized using the internet" (Pilkington and Roberts, 2016: para. 1). This depiction of radicalization as something that happens online often implies the need to find online solutions. Gill et al.'s findings suggest a more nuanced approach is needed.

First and foremost, Gill et al. (2017) give a more complete picture of the particular kinds of information terrorists seek out online. Although the cases are drawn from a sample of individuals from the United Kingdom and therefore may not be wholly generalizable to other contexts, the data show that terrorists looked for ideologically inspired as well as operationally relevant information online. One implication of this finding is that prevention efforts seeking to counter or engage only on terrorists' twisted ideologies may just be part of the solution.

To be sure, there are promising models for challenging radical ideologies online. One example is the Peer to Peer: Challenging Extremism Program, sponsored by U.S. federal agencies including the Departments of Homeland Security and State. The program uses a competition model to engage teams of students from universities around the world to develop and implement social media campaigns to push back on terrorist propaganda (Kaye, 2015). Many campaigns developed by students offer positive messaging, such as by highlighting the contributions of immigrants in society to promote tolerance and understanding (Walsh, 2016). Critics of this approach have sometimes responded that providing specific counter-messages to terrorist propaganda is also necessary (Cottee, 2015).

Examples of initiatives that provide a more direct approach can be seen in the work done by the United Kingdom–based Institute for Strategic Dialogue (ISD). One ISD study aimed to engage with individuals expressing support for violence online. The pilot program enlisted former extremists to reach out through social media platforms to individuals "confirmed to be at risk of falling into the orbit of violent Islamist groups" (Dow and Frenett, 2015: 12). The results showed that messages providing offers of assistance and personalized stories

were most effective at garnering a response from the at-risk individuals. Another ISD study examined three social media campaigns addressing the ideological dimensions of violent extremist groups, including one program working with far right extremists in the United States. This study underscored the potential impact that online counter-messaging efforts can have by "sowing the seeds of doubt" among at-risk populations (Amanullah, Birdwell, Silverman, and Stewart, 2016: 6).

Yet, despite the fact that counter or alternative messaging campaigns show promise, there are still fundamental challenges to address, such as the need to scale up campaigns dramatically to address the volume of information released by terror groups like the Islamic State of Iraq and the Levant (ISIL). Furthermore, as Gill et al. (2017) underscore, "many [violent extremists] went online not to have their beliefs changed but reinforced." This suggests that counter-messaging campaigns addressing ideology alone may not reach or resonate with at-risk individuals. More specifically, as Gill et al. also demonstrate, terrorists used the Internet to plan for many operational aspects of their attack, including searching for online information about how to build bombs or how chemical combinations could be used to inflict harm on others. They also researched potential landmarks to target, and a small number of terrorists "used online resources to help overcome a hurdle they faced in the actual planning of an attack." At present, CVE policies and programs are not usually directed to engage on these operational matters because of the potential for blurring lines between preventative actions and criminal investigation.

A final point to mention with regard to online counterterrorism messaging campaigns relates to the current trend of linking public health models to the field of CVE. Promising practices from public engagement around other public health concerns like suicide prevention may offer insights for developing effective violence prevention campaigns (Eisenman and Weine, 2016). Research on suicide prevention has shown, for instance, that there are important safety gains to be made by removing potential weapons, such as "putting locks on guns, medicine cabinets and drawers containing knives" (Jaffe, 2014: para. 1 of "How to reduce suicide"). Whether analogous actions may be useful for CVE programs remains to be seen. Better understanding of how these kinds of "real-world" preventative actions could be tailored to CVE efforts is needed in addition to continued discussions with technology companies on addressing the spread of terrorist content online (Amanullah and Wiktorowicz, 2015).

Prevention and intervention efforts are still in nascent stages in both the physical and virtual worlds. Currently, policy makers in the United States and Europe are working to develop protocols for offering individually tailored counseling and support mechanisms to at-risk individuals (Vidino and Hughes, 2015). In addition to developing these intervention models, some have also considered how to engage individuals surrounding those at risk for violence. For example, Williams, Horgan, and Evans (2015) found that friends of individuals considering violent actions may be best placed to recognize early warning signs, although friends may be reluctant to report their concerns to law enforcement. Even though the

current study does not directly examine the behaviors and actions of individuals close to those radicalizing, such information could be helpful to assist in the early detection and reporting of potential criminal plots.

Supporting New and Innovative Methodologies for Terrorism Research

Policy makers interested in exploring and supporting CVE programs have repeatedly called for a stronger evidence base to justify CVE program support (Romaniuk, 2015). This need has spurred government funding, albeit in limited amounts, for researchers to improve understanding of whether terrorism prevention works. Academic researchers interested in this work must often resort to obtaining publicly available information via press reports about terrorists and violent extremists, as Gill et al. (2017) did (Dolnik, 2011). Typical data collection techniques include obtaining legal documents like court transcripts warrants, expert witness reports, or in some cases doing ethnographic research. To be clear, these descriptive data points can tell us a good deal about terrorist learning and interaction, and there are comprehensive data sources in the United States such as the Center on National Security at Fordham Law School and the George Washington Program on Extremism that provide case information that is easily accessible to the public and updated frequently. Nevertheless, the limitation of these open-source databases is that they do not contain any classified or "closed-source" materials that are available to law enforcement analysts or the intelligence community. Inside the government, analysts are reluctant to rely solely on open-source information, recognizing that press reporting may be incomplete without classified investigatory information included.

In response, noted terrorism expert Marc Sageman (2014) has called for better integration of academic research and analytical information, observing that most terrorism research is "mostly and secretly conducted within governments, specifically within the [intelligence community], which has not shared much information about terrorist plots with the academic community" (p. 572). In Sageman's view, this has led to a situation where "intelligence analysts know everything but understand nothing, while academics understand everything but know nothing" (p. 576).

Another reason for integrating analysis and research in the field of terrorism is to gain better understanding not only of the terrorists themselves but also of the people around them who may support violence in other ways. In this regard, one area that the Gill et al. (2017) study does not address specifically is the gender dimension. The data examined for this study come from an offender set that is 96% male. This finding, replicated in many studies, has led to a predominate focus on shaping our CVE responses to male offenders (Szmania, 2015).

Yet, there is emerging research illustrating the various roles that women play, namely, in terrorist recruitment and in the dissemination of propaganda (Manrique et al., 2016). These findings point to a need, called for by LaFree (2013), to understand the discrete groups to which violent extremists belong. On a practical level, better understanding of

the varied and distinct roles that individuals, regardless of gender, play in supporting as well as perpetrating acts of violence will help practitioners to tailor CVE prevention and intervention programming efforts, rather than taking a one-size-fits-all approach. By focusing solely on terrorists themselves, we risk overlooking the networks of individuals that support and promulgate terror.

Conclusion

In conclusion, Gill et al.'s (2017) point that policy makers and researchers should shift their focus "from the radicalization process toward an understanding of how crimes are committed" is valid. Understanding the social environments of those who have committed violent crimes will give us a better understanding of how to counter violent extremism in the early stages of an individual's radicalization process. Criminologists, as well as academics from a wide variety of disciplines, have much to add to this work. One question to explore more fully through research is the line between criminal and noncriminal behaviors, although this raises thorny challenges for CVE efforts that typically aim to engage before illegal activity begins. For their part, policy makers must be willing to integrate research findings more fully into their development of policies and programs. This is no easy feat, especially when research findings challenge long held assumptions and hypotheses. Gill et al. (2017), however, show that research can help tease out important nuances in our understanding of the radicalization process online and offline, which ideally can help shape policy responses in efficient and productive ways.

References

Amanullah, Shahed and Quintan Wiktorowicz. 2015. How tech can fight extremism. *CNN.com*. February 17. Retrieved August 3, 2016 from cnn.com/2015/02/16/opinion/wiktorowicz-tech-fighting-extremism/.

Amanullah, Zahed, Jonathan Birdwell, Tanya Silverman, and Christopher J. Stewart. 2016. *The Impact of Counter-Narratives: Insights From a Year-Long Cross-Platform Pilot Study of Counter-Narrative Curation, Targeting, Evaluation and Impact*. London, U.K.: The Institute for Strategic Dialogue.

Cottee, Simon. 2015. Why it's so hard to stop ISIS propaganda. *The Atlantic*. March 2. Retrieved August 5, 2016 from theatlantic.com/international/archive/2015/03/why-its-so-hard-to-stop-isis-propaganda/386216/.

Dolnik, Adam. 2011. Conducting field research on terrorism: A brief primer. *Perspectives on Terrorism*. Retrieved August 5, 2016 from terrorismanalysts.com/pt/index.php/pot/rt/captureCite/dolnik-conducting-field-research/0.

Dow, Moli and Ross Frenett. 2015. *One to One Interventions: A Pilot CVE Methodology*. London, U.K.: The Institute for Strategic Dialogue.

Eisenman, David and Stevan Weine. 2016. How public health can improve initiatives to counter violent extremism. *Start.umd.edu*. April 5. Retrieved August 3, 2016 from start.umd.edu/news/how-public-health-can-improve-initiatives-counter-violent-extremism.

Gill, Paul, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan. 2017. Terrorist use of the Internet by the numbers: Quantifying behaviors, patterns, and processes. *Criminology & Public Policy*, 16: 99–117.

Holmer, Georgia. 2013. *Countering Violent Extremism: A Peacebuilding Perspective*. United States Institute of Peace. August 29. Retrieved September 21, 2016 from usip.org/publications/countering-violent-extremism-peacebuilding-perspective.

Jaffe, D. J. 2014. Preventing suicide in all the wrong ways. *Centerforhealthjournalism.org*. September 9. Retrieved August 3, 2016 from centerforhealthjournalism.org/2014/09/09/preventing-suicide-all-wrong-ways.

Kaye, Kate. 2015. Students, Madison Avenue enlisted in messaging fight against ISIS. *Adage.com*. November 16. Retrieved August 4, 2016 from adage.com/article/news/college-students-buzzfeed-enlisted-messaging-fight-isis/301355/.

LaFree, Gary. 2013. Lone-offender terrorists. *Criminology & Public Policy*, 12: 59–62.

Manrique, Pedro, Zhenfeng Cao, Andrew Gabriel, John Horgan, Paul Gill, Hong Qi, Elvira M. Restrepo, Daniela Johnson, Stefan Wuchty, Chaoming Song, and Neil Johnson. 2016. Women's connectivity in extreme networks. *Sciences Advances*, 2.

Mastroe, Caitlin and Susan Szmania. 2016. *Surveying CVE Metrics in Prevention, Disengagement and De-Radicalization Programs*. Report to the Office of University Programs, Science and Technology Directorate, Department of Homeland Security. College Park, MD: START. Retrieved September 21, 2016 from umd.edu/pubs/START_SurveyingCVEMetrics_March2016.pdf.

Pilkington, Ed and Dan Roberts. 2016. FBI and Obama confirm Omar Mateen was radicalized on the internet. *Theguardian.com*. June 14. Retrieved July 25, 2016 from theguardian.com/us-news/2016/jun/13/pulse-nightclub-attack-shooter-radicalized-internet-orlando.

Romanuik, Peter. 2015. *Does CVE Work? Lessons Learned From the Global Effort to Counter Violent Extremism*. Goshen, IN: Global Center on Cooperative Security. Retrieved September 21, 2016 from globalcenter.org/wp-content/uploads/2015/09/Does-CVE-Work_2015.pdf.

Sageman, Marc. 2014. The stagnation in terrorism research. *Terrorism and Political Violence*, 26: 565–580.

Szmania, Susan. 2015. Broadening the discussion about women and violent extremism. *Start.umd.edu*. June 30. Retrieved August 3, 2016 from start.umd.edu/news/broadening-discussion-about-women-and-violent-extremism.

Vidino, Lorenzo and Seamus Hughes. 2015. *Countering Violent Extremism in America*. Washington, DC: Program on Extremism, Center for Cyber & Homeland Security, The George Washington University.

Walsh, John. 2016. Community College of Aurora wins first Colorado "Peer 2 Peer: Challenging Extremism" competition. *Ise.gov*. May 12. Accessed August 5, 2016 from ise.gov/news/community-college-aurora-wins-first-colorado-%E2%80%9Cpeer-2-peer-challenging-extremism%E2%80%9D-competition.

Williams, Michael J., John G. Horgan, and William P. Evans. 2015. The critical role of friends in networks for countering violent extremism: Toward a theory of

vicarious help-seeking. *Behavioral Sciences of Terrorism and Political Aggression*, 8: 45–65.

United Nations, General Assembly. 2015. *Plan of Action to Prevent Violent Extremism: Report of the Secretary-General* [A/70/674]. Retrieved from un.org/en/ga/search/view_doc.asp?symbol=A/70/674

Susan Szmania is a senior researcher at the University of Maryland's National Consortium for the Study of Terrorism and Responses to Terrorism (START). She is currently detailed to the U.S. Department of Homeland Security through the Science and Technology Directorate, where she is a senior advisor in the Office for Community Partnerships and serves as the chief of research and analysis on the Countering Violent Extremism Task Force.

Phelix Fincher is a graduate of the University of California, Los Angeles College of Letters and Science, with a bachelor's degree in sociology and a minor in gender studies. She was a 2016 summer intern in the Office for Community Partnerships at the U.S. Department of Homeland Security.